

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings of claims in the application:

LISTING OF CLAIMS

1. (Original) A method for remote incremental program verification, said method comprising:
receiving content verified by at least one content provider, said at least one content provider including an applet provider, a device manufacturer and a device issuer, said content including at least one program unit, each program unit comprising an Application Programming Interface (API) definition file and an implementation, each API definition file defining items in its associated program unit that are made accessible to one or more other program units, each implementation including executable code corresponding to said API definition file, said executable code including type specific instructions and data;
installing said content on a resource-constrained device;
disabling subsequent installation of content on said resource-constrained device; and
issuing said resource-constrained device to an end user.
2. (Original) The method of claim 1 wherein said verification is performed by said applet provider.
3. (Original) The method of claim 1 wherein said verification is performed by said device manufacturer.

4. (Original) The method of claim 1 wherein said verification is performed by said device issuer.
5. (Original) The method of claim 1 wherein said verification is performed by said applet provider and said device manufacturer.
6. (Original) The method of claim 1 wherein said verification is performed by said applet provider and said device issuer.
7. (Original) The method of claim 1 wherein said verification is performed by said device manufacturer and said device issuer.
8. (Original) The method of claim 1 wherein said verification is performed by said applet provider, said device manufacturer and said device issuer.
9. (Original) A method for remote incremental program verification, said method comprising:
receiving content verified by at least one content provider, said at least one content provider including an applet provider, a device manufacturer, a device issuer and a trusted post-issuance installer, said content including at least one program unit, each program unit comprising an Application Programming Interface (API) definition file and an implementation, each API definition file defining items in its associated program unit that are made accessible to one or more other program units, each implementation including executable code corresponding to said API definition file, said executable code including type specific instructions and data;
installing said content on a resource-constrained device;
issuing said resource-constrained device to an end user; and

allowing post-issuance installation of verified content on said resource-constrained device by said trusted post-issuance installer, said post-installation occurring after said issuance.

10. (Original) The method of claim 9 wherein said trusted post-issuance installer verifies a new program unit; and said trusted post-issuance installer installs said verified new program unit on said resource-constrained device.
11. (Original) The method of claim 10 wherein post-issuance verification is performed on a resource-rich device.
12. (Original) The method of claim 10 wherein post-issuance verification is performed on a terminal device.
13. (Original) The method of claim 9 wherein said verification is performed by the provider of said new program unit.
14. (Original) The method of claim 9 wherein said verification is performed by said applet provider.
15. (Original) The method of claim 9 wherein said verification is performed by said device manufacturer.
16. (Original) The method of claim 9 wherein said verification is performed by said device issuer.

17. (Original) The method of claim 9 wherein said verification is performed by said applet provider and said device manufacturer.
18. (Original) The method of claim 9 wherein said verification is performed by said applet provider and said device issuer.
19. (Original) The method of claim 9 wherein said verification is performed by said device manufacturer and said device issuer.
20. (Original) The method of claim 9 wherein said verification is performed by said applet provider, said device manufacturer and said device issuer.
21. (Original) The method of claim 9 wherein said verification is performed by said applet provider, said device manufacturer, said device issuer and said trusted post-issuance installer.
22. (Original) The method of claim 9 wherein said verification is performed by said device manufacturer, said device issuer and said trusted post-issuance installer.
23. (Original) The method of claim 9 wherein said verification is performed by said device manufacturer and said trusted post-issuance installer.
24. (Original) The method of claim 9 wherein said verification is performed by said device issuer and said trusted post-issuance installer.
25. (Original) The method of claim 9 wherein post-issuance verification is performed on a resource-rich device.

26. (Original) The method of claim 9 wherein post-issuance verification is performed on a terminal device.
27. (Original) A method for remote incremental program verification, said method comprising:
receiving content verified by at least one content provider, said at least one content provider including an applet provider, a device manufacturer, a device issuer and an untrusted post-issuance installer, said content including at least one program unit, each program unit comprising an Application Programming Interface (API) definition file and an implementation, each API definition file defining items in its associated program unit that are made accessible to one or more other program units, each implementation including executable code corresponding to said API definition file, said executable code including type specific instructions and data;
installing said content on a resource-constrained device;
issuing said resource-constrained device to an end user; and
allowing post-issuance installation of verified content on said resource-constrained device by said untrusted post-issuance installer, said post-installation occurring after said issuance.
28. (Original) The method of claim 27 wherein
said untrusted post-issuance installer verifies a new program unit; and
said untrusted post-issuance installer installs said verified new program unit on said resource-constrained device.
29. (Original) The method of claim 28 wherein post-issuance verification is performed on a resource-rich device.

30. (Original) The method of claim 28 wherein post-issuance verification is performed on a terminal device.
31. (Original) The method of claim 28 wherein said verification is performed by the provider of said new program unit.
32. (Original) The method of claim 27 wherein said verification is performed by said applet provider.
33. (Original) The method of claim 27 wherein said verification is performed by said device manufacturer.
34. (Original) The method of claim 27 wherein said verification is performed by said device issuer.
35. (Original) The method of claim 27 wherein said verification is performed by said applet provider and said device manufacturer.
36. (Original) The method of claim 27 wherein said verification is performed by said applet provider and said device issuer.
37. (Original) The method of claim 27 wherein said verification is performed by said device manufacturer and said device issuer.
38. (Original) The method of claim 27 wherein said verification is performed by said applet provider, said device manufacturer and said device issuer.

39. (Original) The method of claim 27 wherein said verification is performed by said applet provider, said device manufacturer, said device issuer and said untrusted post-issuance installer.
40. (Original) The method of claim 27 wherein said verification is performed by said device manufacturer, said device issuer and said untrusted post-issuance installer.
41. (Original) The method of claim 27 wherein said verification is performed by said device manufacturer and said untrusted post-issuance installer.
42. (Original) The method of claim 27 wherein said verification is performed by said device issuer and said untrusted post-issuance installer.
43. (Original) The method of claim 27 wherein post-issuance verification is performed on a resource-rich device.
44. (Original) The method of claim 27 wherein post-issuance verification is performed on a terminal device.
45. (Original) A program storage device readable by a machine, embodying a program of instructions executable by the machine to perform program verification, comprising: receiving content verified by at least one content provider, said at least one content provider including an applet provider, a device manufacturer and a device issuer, said content including at least one program unit, each program unit comprising an Application Programming Interface (API) definition file and an implementation, each API definition file defining items in its associated program unit that are made accessible to one or more other program units, each

implementation including executable code corresponding to said API definition file, said executable code including type specific instructions and data;
installing said content on a resource-constrained device;
disabling subsequent installation of content on said resource-constrained device; and
issuing said resource-constrained device to an end user.

46. (Original) A program storage device readable by a machine, embodying a program of instructions executable by the machine to perform program verification, comprising:
receiving content verified by at least one content provider, said at least one content provider including an applet provider, a device manufacturer, a device issuer and a trusted post-issuance installer, said content including at least one program unit, each program unit comprising an Application Programming Interface (API) definition file and an implementation, each API definition file defining items in its associated program unit that are made accessible to one or more other program units, each implementation including executable code corresponding to said API definition file, said executable code including type specific instructions and data;
installing said content on a resource-constrained device;
issuing said resource-constrained device to an end user; and
allowing post-issuance installation of verified content on said resource-constrained device by said trusted post-issuance installer, said post-installation occurring after said issuance.

47. (Original) The program storage device of claim 46 wherein
said trusted post-issuance installer verifies a new program unit; and
said trusted post-issuance installer installs said verified new program unit on said resource-constrained device.

48. (Original) The program storage device of claim 47 wherein post-issuance verification is performed on a resource-rich device.
49. (Original) The program storage device of claim 47 wherein post-issuance verification is performed on a terminal device.
50. (Original) The program storage device of claim 46 wherein said verification is performed by the provider of said new program unit.
51. (Original) The program storage device of claim 46 wherein post-issuance verification is performed on a resource-rich device.
52. (Original) The program storage device of claim 46 wherein post-issuance verification is performed on a terminal device.
53. (Original) A program storage device readable by a machine, embodying a program of instructions executable by the machine to perform program verification, comprising: receiving content verified by at least one content provider, said at least one content provider including an applet provider, a device manufacturer, a device issuer and an untrusted post-issuance installer, said content including at least one program unit, each program unit comprising an Application Programming Interface (API) definition file and an implementation, each API definition file defining items in its associated program unit that are made accessible to one or more other program units, each implementation including executable code corresponding to said API definition file, said executable code including type specific instructions and data;
installing said content on a resource-constrained device;
issuing said resource-constrained device to an end user; and

allowing post-issuance installation of verified content on said resource-constrained device by said untrusted post-issuance installer, said post-installation occurring after said issuance.

54. (Original) The program storage device of claim 53 wherein said untrusted post-issuance installer verifies a new program unit; and said untrusted post-issuance installer installs said verified new program unit on said resource-constrained device.
55. (Original) The program storage device of claim 54 wherein post-issuance verification is performed on a resource-rich device.
56. (Original) The program storage device of claim 54 wherein post-issuance verification is performed on a terminal device.
57. (Original) The program storage device of claim 54 wherein said verification is performed by the provider of said new program unit.
58. (Original) A system for executing a software application, the system comprising: a computing system that generates executable code, comprising means for receiving content verified by at least one content provider, said at least one content provider including an applet provider, a device manufacturer and a device issuer, said content including at least one program unit, each program unit comprising an Application Programming Interface (API) definition file and an implementation, each API definition file defining items in its associated program unit that are made accessible to one or more other program units, each implementation including executable code corresponding to said API definition file, said executable code including type specific instructions and data;

means for installing said content on a resource-constrained device;
means for disabling subsequent installation of content on said resource-constrained device; and
means for issuing said resource-constrained device to an end user.

59. (Original) A system for executing a software application, the system comprising:
a computing system that generates executable code, comprising means for receiving content verified by at least one content provider, said at least one content provider including an applet provider, a device manufacturer, a device issuer and a trusted post-issuance installer, said content including at least one program unit, each program unit comprising an Application Programming Interface (API) definition file and an implementation, each API definition file defining items in its associated program unit that are made accessible to one or more other program units, each implementation including executable code corresponding to said API definition file, said executable code including type specific instructions and data;
means for installing said content on a resource-constrained device;
means for issuing said resource-constrained device to an end user; and
means for allowing post-issuance installation of verified content on said resource-constrained device by said trusted post-issuance installer, said post-installation occurring after said issuance.

60. (Original) The system of claim 59 wherein
said trusted post-issuance installer includes a means for verifying a new program unit;
and
said trusted post-issuance installer includes a means for installing said verified new program unit on said resource-constrained device.

61. (Original) The system of claim 60 wherein post-issuance verification is performed on a resource-rich device.
62. (Original) The system of claim 60 wherein post-issuance verification is performed on a terminal device.
63. (Original) The system of claim 59 wherein said verification is performed by the provider of said new program unit.
64. (Original) A system for executing a software application, the system comprising:
a computing system that generates executable code, comprising means for receiving content verified by at least one content provider, said at least one content provider including an applet provider, a device manufacturer, a device issuer and an untrusted post-issuance installer, said content including at least one program unit, each program unit comprising an Application Programming Interface (API) definition file and an implementation, each API definition file defining items in its associated program unit that are made accessible to one or more other program units, each implementation including executable code corresponding to said API definition file, said executable code including type specific instructions and data;
means for installing said content on a resource-constrained device;
means for issuing said resource-constrained device to an end user; and
means for allowing post-issuance installation of verified content on said resource-constrained device by said untrusted post-issuance installer, said post-installation occurring after said issuance.
65. (Original) The system of claim 64 wherein
said untrusted post-issuance installer verifies a new program unit; and

said untrusted post-issuance installer installs said verified new program unit on said resource-constrained device.

66. (Original) The system of claim 65 wherein post-issuance verification is performed on a resource-rich device.

67. (Original) The system of claim 65 wherein post-issuance verification is performed on a terminal device.

68. (Original) The system of claim 65 wherein said verification is performed by the provider of said new program unit.

69. (Original) A resource-constrained device, comprising:
memory for providing content verified by at least one content provider, said at least one content provider including an applet provider, a device manufacturer and a device issuer, said content including at least one program unit, each program unit comprising an Application Programming Interface (API) definition file and an implementation, each API definition file defining items in its associated program unit that are made accessible to one or more other program units, each implementation including executable code corresponding to said API definition file, said executable code including type specific instructions and data; and
a virtual machine that is capable of executing instructions included within said application software program.

70. (Original) The resource-constrained device of claim 69 wherein said resource-constrained device comprises a smart card.

71. (Cancelled)

72. (Original) A resource-constrained device, comprising:

memory for providing content verified by at least one content provider, said at least one content provider including an applet provider, a device manufacturer, a device issuer and a trusted post-issuance installer, said content including at least one program unit, each program unit comprising an Application Programming Interface (API) definition file and an implementation, each API definition file defining items in its associated program unit that are made accessible to one or more other program units, each implementation including executable code corresponding to said API definition file, said executable code including type specific instructions and data;

an installer device for installation of said content on said resource-constrained device, said installation including installation of initial content and installation of additional content by said trusted post-issuance installer after said resource-constrained device is issued to an end user; and

a virtual machine that is capable of executing instructions included within said content.

73. (Original) The resource-constrained device of claim 72 wherein said resource-constrained device comprises a smart card.

74. (Cancelled)

75. (Original) A resource-constrained device, comprising:

memory for providing content verified by at least one content provider, said at least one content provider including an applet provider, a device manufacturer, a device issuer and an untrusted post-issuance installer, said content including at

least one program unit, each program unit comprising an Application Programming Interface (API) definition file and an implementation, each API definition file defining items in its associated program unit that are made accessible to one or more other program units, each implementation including executable code corresponding to said API definition file, said executable code including type specific instructions and data;

an installer device for installation of said content on said resource-constrained device, said installation including installation of initial content and installation of additional content by said untrusted post-issuance installer after said resource-constrained device is issued to an end user; and

a virtual machine that is capable of executing instructions included within said content.

76. (Original) The resource-constrained device of claim 75 wherein said resource-constrained device comprises a smart card.

77. (Cancelled)